SearchSecurity

E-Guide

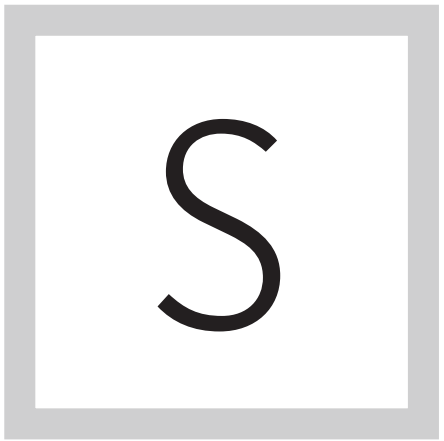
HOW TO GET GREAT RESULTS FROM YOUR AUTHENTICATED VULNERABILITY SCANS

BY KEVIN BEAVER, CISSP

e-guide

TechTarget

SearchSecurity



EARCHSECURITY.COM EXPERT KEVIN Beaver takes you through the five things you can do in order to successfully prepare for, run and get the most out of the results of your authenticated vulnerability scans in this tip.

It's a fact that you cannot secure what you don't acknowledge.

While not exactly a mantra of IT security, this principle certainly proves true when looking for security vulnerabilities from a "trusted" user's perspective. In other words, conducting vulnerability scanning with authentication.

By configuring your vulnerability scanner(s) to log in to the hosts you're testing, you're going to see the rest of the story—the side of security that's often ignored in the name of time, money or complexity. The reality is that running authenticated scans will indeed take more time, but the payoffs in terms of vulnerabilities discovered (and, ultimately, risk mitigated) can be tenfold versus what you would discover otherwise.

Here are five things you can do in order to successfully prepare for, run and get the most out of the results of your authenticated vulnerability scans:

1. Know in advance which systems you're going to scan with authentication. This might include all Windows and Linux-based systems, or a limited subset of your computers (i.e., servers or workstations). Also consider Web applications, databases and any network host that allows or requires authentication via protocols such as Telnet, FTP, SSH and SNMP. Many commercial vulnerability scanners such as Nexpose and

LanGuard provide the ability to scan through various means. If authenticated scanning is common practice used by criminal hackers outside your network or users on the inside (and believe me, it is), then you need to be doing it as well.

2. Decide what user role level (or levels) you want to scan with. I recommend scanning with administrator or root-equivalent credentials at least. You'll find the most flaws this way. However, by scanning with different user roles, such as a manager-level role or basic user role, you can get a better idea of what each user group can see and exploit. The more user roles you test with, the better your results—to an extent. The law of diminishing returns will kick in at some point. You'll know when enough is enough when you see that your results are no longer varying by permissions.

3. Set up the user accounts to be used for authenticated scanning to not force a password change upon initial login (a common setting in Active Directory Group Policies and some Web applications). If you forget this, the first time your scanner logs in it will be prompted to change the

password which, of course, it won't be able to do. You may be unaware that this has taken place and then proceed with the scan. Several minutes—or more likely hours—later you'll realize that authentication didn't work and you'll have to start your scans over. With Web vulnerability scanners, you'll likely have to create a login macro that you'll be able to test. For some reason most network vulnerability scanners don't provide an option to test your login credentials before you start scanning. The only two scanners I've ever known to have this feature are the old Harris STAT Scanner and Rapid7's Nexpose. It may seem trite, but this feature can save you massive amounts of time and hassle over the long haul.

4. Authenticated vulnerability scans of network hosts are fairly benign. That said, they can be problematic for production environments, especially when scanning Web applications. Regardless of what you're scanning, CPU, disk and network cycles will be consumed, log files and databases can get filled up, user accounts can get locked out, and so on. I recommend running your authenticated scans on one or two systems at first to see what the side effects are going to be before branching out and scanning hundreds or thousands of systems.

5. The security vulnerabilities uncovered during authenticated scans can be downright overwhelming, especially when viewing the results in a traditional PDF report. I've found that generating HTML or spreadsheet reports, sorted by vulnerability, is the best way to view the findings. When you sort your results by vulnerability, you'll save a ton of time by being able to see things more simply and clearly (i.e., which hosts or Web pages are affected by each vulnerability) and can generate your final report or remediation plans more easily that way, rather than looking at one host at a time.

Using a vulnerability scanner to perform vulnerability scans the right way is similar to using a digital SLR camera to take photos. Anyone can own the tool but it doesn't mean you know how to use it well, and there's no guarantee of positive results. The more you perform your authenticated scans, the more tricks you'll learn that will make you more effective and efficient. Your ability to find vulnerabilities better in a shorter period of time will increase while your business risks can be reduced. Everyone wins.

SearchSecurity

KEVIN BEAVER is an information security consultant, writer, professional, speaker and expert witness at Atlanta-based Principle Logic, LLC. With over 25 years of experience in the industry, Kevin specializes in performing independent security vulnerability assessments of network systems as well as Web and mobile applications. He has authored or co-authored 11 books on information security, including the best-selling Hacking For Dummies, The Practical Guide to HIPAA Privacy and Security Compliance and Implementation Strategies for Fulfilling and Maintaining IT Compliance. In addition, he's the creator of the Security On Wheels information security audio books and blog, providing security learning for IT professionals on the go. You can reach Kevin through his website www.principlelogic.com and follow him on Twitter at @kevinbeaver.

SearchSecurity

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.